UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/642,625	08/18/2000	Peter A.J. van der Made	81924.0001	8243

7590 10/28/2003

W. SCOTT PETTY
KING & SPALDING
191 PEACHTREE STREET
45TH FLOOR
ATLANTA, GA 30303-1763

EXAMINER	
KISS, ERIC B	

ART UNIT	PAPER NUMBER
2122	

DATE MAILED: 10/28/2003

17

Please find below and/or attached an Office communication concerning this application or proceeding.

3

Office Action Summary	Application No.	Applicant(s)	
	09/642,625	VAN DER MADE, PETER A.J.	
	Examiner	Art Unit	
	Eric B. Kiss	2122	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2003* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *13,14* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. The amendment of July 23, 2003, has been received and entered. Claims 1-25 are pending.

Response to Amendment

2. Applicant's amendments to the specification appropriately address the objection to the specification as detailed in the previous office action. Accordingly, this objection is withdrawn in view of Applicant's amendments.

3. Applicant's amendments to the claims appropriately address the rejections of claims 3, 5, 9, and 16 under 35 U.S.C. §112, second paragraph, as detailed in the previous office action. Accordingly, these rejections are withdrawn in view of Applicant's amendments. Note, however, the new rejection of claims 6-9 and 13-17 under 35 U.S.C. §112, second paragraph, introduced below.

Response to Arguments

4. Applicant's arguments with respect to claims 1-25 have been considered but are moot in view of the new grounds of rejection. The new grounds of rejection presented below are necessitated by Applicant's amendments to the claims.

Claim Rejections - 35 USC § 112

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 6-9 and 13-17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a) Claim 6 recites the limitation "wherein after a first instance of a first program is analyzed by the virtual machine and a first behavior pattern is generated and stored in a database coupled to the computer system..." in lines 1-3. There is insufficient antecedent basis for this limitation in the claim. In the interest of compact prosecution, the preamble elements lacking antecedent basis are subsequently ignored, and "first program" is subsequently interpreted as "target program" for the purpose of further examination.

b) Claims 7-9 are rejected based on the inherited parent claim limitation recited in claim 6 and rejected as set forth above.

c) Claim 13 recites the limitation "wherein after a first instance of a first program is analyzed by the virtual machine and a first behavior pattern is generated and stored in a database coupled to the computer system..." in lines 1-3. There is insufficient antecedent basis for this limitation in the claim. In the interest of compact prosecution, the preamble

elements lacking antecedent basis are subsequently ignored, and "first program" is subsequently interpreted as "target program" for the purpose of further examination.

d) Claims 14-17 are rejected based on the inherited parent claim limitation recited in claim 13 and rejected as set forth above.

Claim Rejections - 35 USC § 103

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 1, 5, 11, 12, 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Understanding Heuristics: Symantec's Bloodhound Technology," 1997 (hereinafter *UHSBT*) in view of Robert Richardson, "Enterprise Anti-Virus Software," February 2000 (hereinafter *Richardson*).

a) As per claim 1, *UHSBT* discloses:

initializing a virtual machine within a computer system, the virtual machine comprising a virtual personal computer (PC) implemented by software simulating functionality of a central processing unit and memory and a virtual operating system simulating functionality of an operating system of the computer system (see, for example, page 6, paragraphs 4-5);

virtually executing a target program within the virtual PC so that the target program interacts only with an instance of the virtual operating system (see, for example, page 6, paragraphs 4-5);

analyzing behavior of the target program upon completion of virtual execution to identify an occurrence of malicious code behavior based upon evaluation by the virtual machine of a behavior pattern representing information about all functions simulated by the target program during virtual execution (see, for example, page 8, paragraph 3); and

terminating the virtual PC after the analyzing process, thereby removing from the computer system a copy of the target program that was contained within the virtual PC (inherent).

UHSBT fails to expressly disclose the virtual operating system simulating functionality of a multi-threaded operating system. However, *Richardson* teaches that it is known to employ a virtual operating system simulating functionality of a multi-threaded operating system (*a WINDOWS emulator*; see page 2, paragraph 8) as part of a dynamic heuristic approach to virus scanning. Note that the teachings of *Richardson* incorporate quotations from Carey Nachenberg, chief researcher at the Symantic AntiVirus Research Center, developers of the system disclosed in *UHSBT*. Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to modify the system of *UHSBT* to include, if not already provided, a virtual operating system simulating functionality of a multi-threaded operating system. One would be motivated to do so to entice a virus to reveal behavior specifically designed for such a multi-threaded operating system to aid in detection of such a virus.

b) As per claim 5, *UHSBT* further discloses the target program being newly introduced to the computer system and initially executed by virtually executing the target program on the virtual PC (As is well known in the art, virus scanning tools, such as the tool disclosed by *UHSBT* are primarily used to protect a system from viruses; *UHSBT* discloses that it is desirable to detect viruses before they have a chance to run and infect a computer system; see, for example, page 3, paragraphs 3-4). Therefore, for reasons stated above, such a claim also would have been obvious.

c) As per claim 11, *UHSBT* discloses:

initializing a virtual machine within a computer system, the virtual machine comprising software simulating functionality of a central processing unit and memory (see, for example, page 6, paragraphs 4-5);

virtually executing a target program with the virtual PC so that the target program interacts with an instance of the virtual operating system rather that with the operating system of the computer system, whereby the malicious code is fully executed during virtual execution of the target program if the target program comprises the malicious code (see, for example, page 6, paragraphs 4-5);

generating a behavior patter for the target program to collect information about all functions simulated by the target program during virtual execution (see, for example, page 8, paragraph 3); and

terminating the virtual machine upon completion of the virtual execution of the target program, leaving behind a record of the behavior pattern that is representative of operations of the target program with the computer system, including operations of the

malicious code if the target program comprises the malicious code (see, for example, page 6, paragraph 5; and page 8, paragraph 3).

UHSBT fails to expressly disclose the virtual operating system simulating functionality of a multi-threaded operating system. However, *Richardson* teaches that it is known to employ a virtual operating system simulating functionality of a multi-threaded operating system (*a WINDOWS emulator*; see page 2, paragraph 8) as part of a dynamic heuristic approach to virus scanning. Note that the teachings of *Richardson* incorporate quotations from Carey Nachenberg, chief researcher at the Symantic AntiVirus Research Center, developers of the system disclosed in *UHSBT*. Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to modify the system of *UHSBT* to include, if not already provided, a virtual operating system simulating functionality of a multi-threaded operating system. One would be motivated to do so to entice a virus to reveal behavior specifically designed for such a multi-threaded operating system to aid in detection of such a virus.

d) As per claim 12, *UHSBT* further discloses the record being in a behavior register in the computer system (see, for example, page 6, paragraph 5; and page 8, paragraph 3). Therefore, for reasons stated above, such a claim also would have been obvious.

e) As per claims 18 and 20, *UHSBT* discloses:

initializing a virtual machine within a computer system, the virtual machine comprising software simulating functionality of a central processing unit and memory (see, for example, page 6, paragraphs 4-5);

virtually executing a target program with the virtual PC so that the target program interacts with an instance of the virtual operating system rather that with the operating system of the computer system, whereby the malicious code is fully executed during virtual execution of the target program if the target program comprises the malicious code (see, for example, page 6, paragraphs 4-5);

generating a behavior patter for the target program to collect information about all functions simulated by the target program during virtual execution (see, for example, page 8, paragraph 3); and

upon completion of the virtual execution of the target program, comparing the behavior pattern generated by the virtual machine to a behavior pattern representative of malicious code and identifying malicious code if the comparison results in a match (see, for example, page 6, paragraph 5; and page 8, paragraph 3).

UHSBT fails to expressly disclose the virtual operating system simulating functionality of a multi-threaded operating system. However, *Richardson* teaches that it is known to employ a virtual operating system simulating functionality of a multi-threaded operating system (*a WINDOWS emulator*; see page 2, paragraph 8) as part of a dynamic heuristic approach to virus scanning. Note that the teachings of *Richardson* incorporate quotations from Carey Nachenberg, chief researcher at the Symantic AntiVirus Research Center,

developers of the system disclosed in *UHSBT*. Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to modify the system of *UHSBT* to include, if not already provided, a virtual operating system simulating functionality of a multi-threaded operating system. One would be motivated to do so to entice a virus to reveal behavior specifically designed for such a multi-threaded operating system to aid in detection of such a virus.

f) As per claims 19 and 21, in addition to the disclosure and teachings applied above, although *UHSBT* fails to expressly disclose removing the target program from the computer system in response to detection of malicious code, Official Notice is taken that it has been known and practices to remove undesirable programs from a system to prevent execution, accidental or intentional, of those undesirable programs. Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to include removing programs comprising detected malicious code from the computer system. One would be motivated to do so to protect the computer system from undesirable effects associated with execution of malicious code.

g) As per claims 22-25, see the disclosure and teachings applied above to claims 18 and 19. For reasons stated above, such claims also would have been obvious.

9. Claims 2-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over *UHSBT* in view of *Richardson* as applied to claim 1 above, and further in view of U.S. Patent No. 6,275,938 B1 to Bond et al.

a) As per claims 2 and 4, in addition to the disclosure and teachings applied above to claim 1, *UHSBT* further discloses the virtual PC simulating functionality of input/output ports (for example, interrupt requests), and the virtual operating system simulating functionality of operating system data areas (for example, page 6, paragraphs 4-5). *UHSBT* fails to expressly disclose the virtual operating system simulating functionality of an operating system application program interface, wherein virtual execution of the target program causes the target program to interact with the simulated operating system application program interface. However, *Bond et al.* teach, as part of a secure software execution environment (sandbox), remapping API calls from untrusted software to secure routines, including simulated APIs, such as allocation APIs that are capable of allocating memory only within the sandbox, and simulating error returns for APIs which are to be blocked entirely (see, for example, column 6, line 24, through column 7, line 9). Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to further modify the system of *UHSBT* to include simulating an application program interface and causing the target program to interact with the simulated application program interface as per the teachings of *Bond et al.* One would be motivated to do so to prevent untrusted code from having complete, unsecured, control of the operating system while still allowing the untrusted code to execute.

b) As per claim 3, *UHSBT* and *Richardson* disclose/teach such a method (see the disclosure and teachings applied to claim 1 above) but fail to expressly disclose the virtual operating system being operative to simulate an application program interface call of the operating system by returning a correct value to the call without completing actual performance of the call. However, *Bond et al.* teach, as part of a secure software execution environment (sandbox), remapping API calls from untrusted software to secure routines, including simulated APIs, such as allocation APIs that are capable of allocating memory only within the sandbox, and simulating error returns for APIs which are to be blocked entirely (see, for example, column 6, line 24, through column 7, line 9). Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to further modify the system of *UHSBT* to include simulating an application program interface call of the operating system by returning a correct value to the call without completing actual performance of the call as per the teachings of *Bond et al.* One would be motivated to do so to prevent untrusted code from having complete, unsecured, control of the operating system while still allowing the untrusted code to execute.

10. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over *UHSBT* in view of *Richardson* as applied to claim 1 above, and further in view of Baudouin Le Charlier et al., "Dynamic Detection and Classification of Computer Viruses Using General Behavior Patterns," 1995 (hereinafter *Le Charlier et al.*).

a) As per claim 10, in addition to the disclosure and teachings applied above to claim 1, *UHSBT* further discloses the behavior pattern identifying functions executed in the virtual execution of the target program (see, for example, page 8, paragraphs 3-5) but fails to expressly disclose tracking an order in which the functions are virtually executed by the target program within the virtual PC to provide a complete record of all functions simulated by the target program, as if the target program were executed on the computer system. However, *Le Charlier et al.* teach tracking an order in which the functions are virtually executed by the target program within an emulator to provide a complete record of all functions simulated by the target program (see, for example, sections 4.5 and 4.6). Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to further modify the system of *UHSBT* to include tracking an order in which the functions are virtually executed by the target program within an emulator as per the teachings of *Le Charlier et al.* One would be motivated to do so to be able to model virus activity as a set of rules related to state transitions to capture dynamic behavior of a virus.

11. Claims 6-9 and 13-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over *UHSBT* in view of *Richardson* as applied to claim 1 above, and further in view of Jeffrey O. Kephart, et al., "Blueprint for a Computer Immune System," 1997 (hereinafter *Kephart et al.*).

a) As per claims 6-9 and 13-16, *UHSBT* and *Richardson* fail to expressly disclose determining that the target program is modified; analyzing the modified program to

provide a second behavior pattern; comparing the behavior pattern to the second behavior pattern to determine if malicious code is present in the modified program; generating a new behavior pattern each time the target program is modified; identifying altered bits indicating an addition of an infection procedure; or identifying the behavior pattern as a match to the second behavior pattern when the modified target program is a new version of the target program. However, *Kephard et al.* teach determining that a program is modified (see, for example, section 3.1.1); analyzing the modified program to provide a behavior pattern (see, for example, section 3.1.1); comparing the behavior pattern to a previous known behavior pattern to determine if malicious code is present in the modified program (see, for example, section 3.1.1); generating a new behavior pattern each time the program is modified (see, for example, section 3.1.1); identifying altered bits indicating an addition of an infection procedure (see, for example, section 3.1.1); and identifying when the modified program is a new version of the target program (see, for example, section 3.1.1). Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to further modify the system of *UHSBT* to include such modified behavior determination and analysis as per the teachings of *Kephart et al.* One would be motivated to do so to be able to detect whether changes in a program are due to malicious code being present.

12. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over *UHSBT* in view of *Richardson* and *Kephart et al.* as applied to claim 13 above, and further in view of *Le Charlier et al.* as applied to claim 10 above.

a) As per claim 17, in addition to the disclosure and teachings applied above to claims 6-9 and 13-16, see the disclosure and teachings applied above to claim 10. For reasons stated above, such a claim also would have been obvious.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

15. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Eric B. Kiss whose telephone number is (703) 305-7737. The Examiner can normally be reached on Tue. - Fri., 7:30 am - 5:00 pm. The Examiner can also be reached on alternate Mondays.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Tuan Dam, can be reached on (703) 305-4552. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

EBK
October 16, 2003

TUAN DAM
SUPERVISORY PATENT EXAMINER